PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-306092
(43)Date of publication of application : 05.11.1999

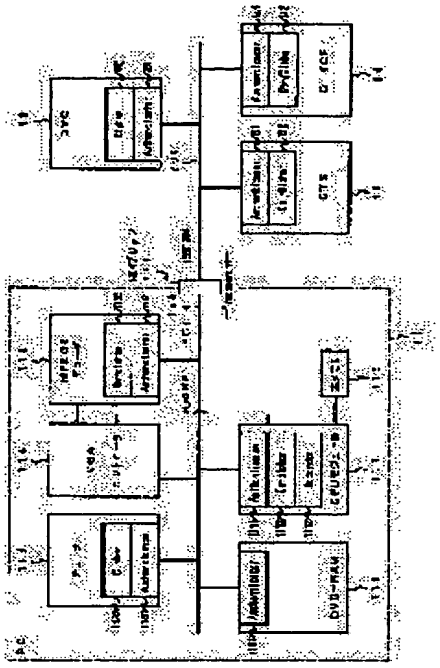
(51)Int.Cl. G06F 12/16
G06F 12/14

(21)Application number : 10-108116
(22)Date of filing : 17.04.1998

(71)Applicant : TOSHIBA CORP
(72)Inventor : ISHIBASHI YASUHIRO
SOGABE HIDEKI

(54) DATA PROCESSOR AND COPY PROTECT SYSTEM APPLIED TO THE PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide protection of digital contents flowing on a bus of a computer system and limit of the digital contents for each function module.
SOLUTION: With regard to a CPU module 111, a tuner 113 for a satellite or digital TV, an MPEG 2 decoder 115, and a DVD-RAM drive 116, an interface part with a PCI bus 100 is provided with authentication processing parts (authenticators) 1111, 1131, 1151 and 1161 for performing equipment authentication, key exchange and the like. In this way, providing each function module with a authentication function for enciphering processing, it becomes possible to efficiently realize protection of digital contents flowing on the PCI bus 200 connecting between the function modules, and limit of the digital contents for each function module.



LEGAL STATUS

[Date of request for examination]	24.03.2000
[Date of sending the examiner's decision of rejection]	09.07.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3361052
[Date of registration]	18.10.2002
[Number of appeal against examiner's decision of rejection]	2002-014993
[Date of requesting appeal against examiner's decision of rejection]	08.08.2002
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－306092

(43)公開日　平成11年(1999)11月５日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	12/16	３２０	Ｇ０６Ｆ	12/16	３２０Ｂ
					３２０Ｅ
	12/14	３２０		12/14	３２０Ｂ
					３２０Ｅ

審査請求　未請求　請求項の数16　ＯＬ　（全 19 頁）

(21)出願番号　特願平10－108116

(22)出願日　平成10年(1998)４月17日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

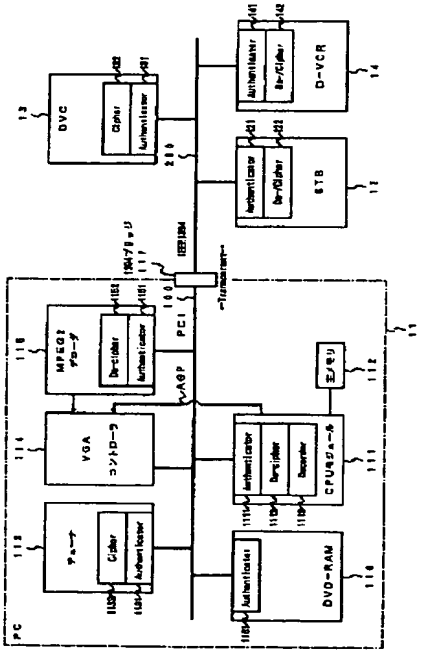
(72)発明者　石橋　泰博
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

(72)発明者　曽我部　秀樹
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　データ処理装置および同装置に適用されるコピープロテクト方法

(57)【要約】
【課題】コンピュータシステムのバス上に流れるデジタルコンテンツの保護と、機能モジュール単位でのデジタルコンテンツの制限を実現する。
【解決手段】ＣＰＵモジュール１１１、サテライトまたはデジタルＴＶ用のチューナ１１３、ＭＰＥＧ２デコーダ１１５、ＤＶＤ－ＲＡＭドライブ１１６については、ＰＣＩバス１００とのインターフェイス部に、機器認証およびキー交換などを行う認証処理部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）１１１１，１１３１，１１５１，１１６１が設けられている。このように機能モジュールそれぞれに暗号化処理のための認証機能を設けることにより、機能モジュール間を接続するＰＣＩバス２００上に流れるデジタルコンテンツの保護と、機能モジュール単位でのデジタルコンテンツの制限を効率よく実現できるようになる。



1

【特許請求の範囲】

【請求項１】　コピープロテクト対象のデータを暗号化して授受するための認証機能を有する外部機器が接続可能な外部バスとのインターフェイスを有するデータ処理装置において、

内部バスと、

この内部バスにそれぞれ結合され、コピープロテクト対象のデータを前記内部バス経由で送信または受信する複数の機能モジュールと、

前記各機能モジュール毎に設けられ、前記コピープロテクト対象のデータを授受する相手先の機能モジュールまたは前記外部機器との間で、前記コピープロテクト対象のデータを暗号化して授受するための認証処理を行う認証手段とを具備し、

前記データ処理装置内の各機能モジュール毎に認証処理を行うことを特徴とするデータ処理装置。

【請求項２】　前記内部バスを介して前記コピープロテクト対象のデータを送信する送信側の機能モジュールには、前記コピープロテクト対象のデータを暗号化する暗号化手段が設けられ、且つ前記バスを介して前記コピープロテクト対象のデータを受信および処理する受信側の機能モジュールには、前記暗号化されたデータを復号化してその暗号化を解除するための復号化手段が設けられていることを特徴とする請求項１記載のデータ処理装置。

【請求項３】　前記外部バスと前記内部バスとの間を透過的に接続する外部バスインターフェイス手段をさらに具備し、

前記外部機器と前記各機能モジュールとの間でコピープロテクト対象のデータを授受するとき、前記外部バスおよび内部バス上には暗号化データが転送され、

前記機能モジュール相互間、および前記外部機器と前記機能モジュールとの間の双方で、同一の認証および暗号化プロトコルが使用されることを特徴とする請求項２記載のデータ処理装置。

【請求項４】　前記コピープロテクト対象のデータを扱う機能モジュールにには、ＣＰＵモジュール、デジタル圧縮符号化された符号化データをデコードするデコーダ、およびストレージデバイスの内の少なくとも一つが含まれていることを特徴とする請求項１記載のデータ処理装置。

【請求項５】　前記コピープロテクト対象のデータの種類には一回のみコピー可のデータと、コピー不可のデータとがあり、前記各機能モジュールには、その機能モジュールが扱うことが可能なデータの種類を規定するための識別情報が割り当てられており、

前記認証手段は、

受信側の機能モジュールに対応する識別情報に基づいてその受信側の機能モジュールが送信対象のデータを扱うことが可能な機能モジュールであるか否かを判別し、送

2

信対象のデータを扱うことが可能な機能モジュールであるとき、暗号化データを復号化するために必要な暗号化解除キーを受信側の機能モジュールに生成させるためのキー交換を受信側の機能モジュールとの間で実行することを特徴とする請求項１記載のデータ処理装置。

【請求項６】　暗号化されたデータを復号化するために必要な暗号化解除キーは送信対象のデータの種類毎に変更され、

種類の異なる複数種のデータから構成されるストリームを送信するとき、前記認証処理によって、前記ストリームを構成するデータの種類の中で受信側の機能モジュールが処理可能なデータの種類数に対応する数の暗号化解除キーが前記受信側の機能モジュール上に生成されることを特徴とする請求項１記載のデータ処理装置。

【請求項７】　前記ストリームにはデータの種類を示すデータ種別情報が埋め込まれており、

前記受信側の機能モジュールは、前記データ種別情報に基づいて、使用する暗号化解除キーを動的に変更することを特徴とする請求項６記載のデータ処理装置。

【請求項８】　前記データ処理装置は、前記機能モジュールとしてＣＰＵモジュール、デジタル圧縮符号化された符号化データをデコードするデコーダ、およびストレージデバイスを有するパーソナルコンピュータであり、このパーソナルコンピュータは前記内部バスとしてＰＣＩバスを有し、前記外部バスとしてＩＥＥＥ１３９４シリアルバスを有することを特徴とする請求項１記載のデータ処理装置。

【請求項９】　バスと、このバスにそれぞれ結合された複数の機能モジュールとを有するデータ処理装置において、

前記複数の機能モジュールの中でコピープロテクト対象のデジタルコンタンツを扱う各機能モジュールは、前記バスを介してデジタルコンタンツを授受する相手先の機能モジュールとの間で、前記デジタルコンタンツを暗号化して授受するための認証処理を行う認証手段を具備し、

前記コピープロテクト対象のデジタルコンテンツの種類には一回のみコピー可のコンテンツと、コピー不可のコンテンツとがあり、前記各機能モジュール毎に、その機能モジュールが扱うことが可能なコンテンツの種類が規定されており、

前記認証手段は、

受信側の各機能モジュール毎にその機能モジュールが送信対象のコンテンツを扱うことが可能な機能モジュールであるか否かを判別することを特徴とするデータ処理装置。

【請求項１０】　内部バスと、この内部バスにそれぞれ結合され、コピープロテクト対象のデータを前記内部バス経由で送信または受信する複数の機能モジュールと、コピープロテクト対象のデータの暗号化／復号化機能を

有する外部機器が接続可能な外部バスと前記内部バスとの間を接続する外部バスインターフェイス手段とを具備するデータ処理装置に適用されるコピープロテクト方法において、
前記外部バスインターフェイス手段によって前記外部バスと前記システムバスとの間を透過的に接続し、
前記複数の機能モジュール相互間あるいは前記機能モジュールと外部機器との間でコピープロテクト対象のデータを授受するとき、通信対象のデバイス相互間で互いの機能モジュールの正当性を確認するための認証処理を実行し、
この認証処理で互いのデバイスの正当性が確認されたとき、送信側のデバイスにて送信データを暗号化して相手先のデバイスに送信し、
その暗号化データを受信側のデバイスにて復号化し、
前記システムバス上に流れるデータと前記外部バスに流れるデータの双方を、コピープロテクトすることを特徴とするコピープロテクト方法。

【請求項１１】　バスと、このバスに接続された複数のデバイスとから構成されるシステムに適用されるデジタルコンテンツのコピープロテクト方法であって、
種類の異なる複数種のデジタルコンテンツから構成されるストリームを暗号化して受信側のデバイスに送信するとき、送信側のデバイスは、その送信に先だって、受信側のデバイス毎にそれが扱うことができるコンテンツの種類数だけ認証処理を行うことにより、前記ストリームを構成するデジタルコンテンツの種類の中で受信側のデバイスが処理可能なデータの種類数に対応する暗号化解除キーを各受信側のデバイスに通知し、
受信側のデバイスは、受信したデジタルコンテンツの種類に応じて、使用する暗号化解除キーを変更することを特徴とするコピープロテクト方法。

【請求項１２】　前記ストリームにはデジタルコンテンツの種類を示す種別情報が埋め込まれており、
受信側のデバイスは、前記データ種別情報に基づいて、復号化処理に使用する暗号化解除キーを動的に変更することを特徴とする請求項１１記載のコピープロテクト方法。

【請求項１３】　内部バス上に流されるデジタルコンテンツの不正なコピーを防止するように受信装置側にデータを送信するデータ処理装置において、
前記受信装置との間でコピープロテクト対象のデータの処理が許可されているか否かを認証する認証手段と、
前記認証手段により認証された場合、前記受信装置が処理を許可されているコピープロテクト対象のデータが、どのような種類のデジタルコンテンツであるかを判別する判定手段と、
この判定手段の判定結果に基づいて、前記受信装置が処理を許可されているデジタルコンテンツの種類にそれぞれ対応する暗号化解除キーを前記受信装置に送信するキー送信手段と、
前記暗号化解除キーを利用して前記受信装置が暗号を解除できるデジタルコンテンツを送信する送信手段とを具備したことを特徴とするデータ処理装置。

【請求項１４】　コンピュータシステムの内部バス上に流されるデジタルコンテンツの不正なコピーを防止するよう、受信装置側にデータを適正に送信するコピープロテクト方法であって、
前記受信装置との間でコピープロテクト対象のデータの処理が許可されているか否かを認証し、
認証された場合、前記受信装置が処理を許可されているコピープロテクト対象のデータが、どのような種類のデジタルコンテンツであるかを判別し、
この判定結果に基づいて、前記受信装置が処理を許可されているデジタルコンテンツの種類にそれぞれ対応する暗号化解除キーのみを前記受信装置に送信し、
この暗号化解除キーを利用して前記受信装置が暗号を解除できるデジタルコンテンツを送信することを特徴とするコピープロテクト方法。

【請求項１５】　内部バス上に流されるデジタルコンテンツの不正コピーを防止するように送信装置側から送信されたデータを受信処理するデータ処理装置において、
前記送信装置との間でコピープロテクト対象のデータの処理が許可されているか否かを認証する認証手段と、
前記認証手段により認証された場合、このデータ処理装置が処理を許可されているコピープロテクト対象のデジタルコンテンツの種類を示す情報を前記送信装置に送信する種類情報送信手段と、
この種類情報に基づいて前記データ処理装置が処理を許可されているコピープロテクト対象のデジタルコンテンツの種類にそれぞれ対応する暗号化解除キーと、この暗号化解除キーを利用して前記データ処理装置が暗号を解除できるデジタルコンテンツとを、前記送信装置から受け取り、前記デジタルコンテンツを復号化する復号化手段とを具備したことを特徴とするデータ処理装置。

【請求項１６】　コンピュータシステムの内部バス上に流されるデジタルコンテンツの不正なコピーを防止するように、送信装置側から適正にデータを受信処理するコピープロテクト方法であって、
前記送信装置との間でコピープロテクト対象のデータの処理が許可されているか否かを認証し、
認証された場合、データの受信処理を許可されているコピープロテクト対象のデジタルコンテンツの種類を示す情報を前記送信装置に送信し、
この種類情報に基づいて、前記受信処理を許可されているデジタルコンテンツの種類にそれぞれ対応する暗号化解除キーを前記送信装置より受け取り、
この暗号化解除キーを利用して受信装置が暗号を解除できるデジタルコンテンツを、前記送信装置から受け取り、

前記デジタルコンテンツを前記暗号化解除キーを利用して復号化することを特徴とするコピープロテクト方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はパーソナルコンピュータなどのデータ処理装置および同装置で使用されるデジタルコンテンツのコピープロテクト方法に関し、特にＩＥＥＥ１３９４シリアルバスなどの外部バスとのインターフェイスを有するデータ処理装置および同装置に適用されるコピープロテクト方法に関する。

【０００２】

【従来の技術】近年、コンピュータ技術の発達に伴い、デジタルビデオプレーヤ、セットトップボックス、ＴＶ、パーソナルコンピュータ等のマルチメディア対応の電子機器が種々開発されている。

【０００３】この種の電子機器は、例えばＤＶＤ（Ｄｉｇｉｔａｌ　ＶｅｒｓａｔｉｌｅＤｉｓｋ）に蓄積された映画、デジタル衛星放送によるＴＶ番組等のデジタルコンテンツを再生することができる。

【０００４】デジタルコンテンツは一般にＭＰＥＧ２という動画像高能率符号化方式を使って符号化された後、記録媒体や、伝送媒体を通じて各家庭に送られる。ＭＰＥＧ２による符号化は、画質と、容量に対する記録時間の双方を確保する観点から、可変レート符号化の考えに基づいている。可変レート符号化データのデータ量は、元の画像の画質に依存し、動きの激しいシーンほどそのデータ量は増加する。よって、デジタルコンテンツは、各家庭にオリジナル映像と遜色のない高画質の映像を提供することができる。

【０００５】近年、このようなデジタルコンテンツの著作権保護等の観点から、その不正コピーを防止するためのコピープロテクト技術の必要性が叫ばれてきたが、有効な手法が構築されていないのが現状である。

【０００６】そこで、ＣＰＴＷＧ（Ｃｏｐｙ　Ｐｒｏｔｅｃｔｉｏｎ　ＴｅｃｈｎｉｃａｌＷｏｒｋｉｎｇ　Ｇｒｏｕｐ）では、マルチメディアデータの伝送に好適な次世代のバスインターフェイスであるＩＥＥＥ１３９４シリアルバスに向けた新たなコピープロテクト方式の仕様（以下、ＩＥＥＥ１３９４コピープロテクト技術と称する）の策定作業が進められている。

【０００７】ＩＥＥＥ１３９４シリアルバスは、デジタルビデオプレーヤ、セットトップボックス、ＴＶ、パーソナルコンピュータ等をつなぐ次世代のバスインターフェイスであり、転送モードとして、アシンクロナス　サブアクションと、アイソクロナス　サブアクションの２種類をサポートしている。前者は、非同期転送モードと呼ばれ、リアルタイム性が要求されない一般のデータの転送時に使用される。後者は、転送帯域を保証した同期転送モードであり、ビデオデータやオーディオデータに代表されるデジタルコンテンツのリアルタイム転送が可能である。

【０００８】ＩＥＥＥ１３９４コピープロテクト技術は、公開鍵暗号化方式や共通鍵暗号化方式などのよく知られた暗号化プロトコルを用いることにより、ＩＥＥＥ１３９４シリアルバスを介してデジタルビデオプレーヤ、セットトップボックス、ＴＶ、パーソナルコンピュータなどの機器間で受け渡しされるデジタルコンテンツを暗号化し、その不正コピーを防止できるようにしている。

【０００９】

【発明が解決しようとする課題】しかし、パーソナルコンピュータはもともとオープンなシステムであるため、ＩＥＥＥ１３９４シリアルバス上に流れるデータを暗号化しただけでは、不正コピーに対する十分な保護を期待することはできない。以下、これについて具体的に説明する。

【００１０】図１５は、ＩＥＥＥ１３９４コピープロテクト技術をそのままパーソナルコンピュータに適用した場合の構成例である。図１５においては、パーソナルコンピュータ（ＰＣ）１、セットトップボックス（ＳＴＢ）２、およびデジタルビデオカメラ（ＤＶＣ）３の３つの機器がＩＥＥＥ１３９４シリアルバス１０を介して接続されている様子が示されている。

【００１１】これらパーソナルコンピュータ（ＰＣ）１、セットトップボックス（ＳＴＢ）２、およびデジタルビデオカメラ（ＤＶＣ）３は、それぞれＩＥＥＥ１３９４シリアルバス１０とのインターフェイス部に、暗号化部（Ｃｉｐｈｅｒ）、復号化部（Ｄｅ－Ｃｉｐｈｅｒ）、または暗号化・復号化双方の機能を持つ暗号化／復号化部（Ｄｅ－／Ｃｉｐｈｅｒ）を有している。

【００１２】すなわち、ＩＥＥＥ１３９４シリアルバス１０を介して他の機器にデジタルコンテンツの送信を行うデジタルビデオカメラ（ＤＶＣ）３については暗号化部（Ｃｉｐｈｅｒ）が設けられ、ＩＥＥＥ１３９４シリアルバス１０を介して他の機器との間でデジタルコンテンツの送受信を行うパーソナルコンピュータ（ＰＣ）１およびセットトップボックス（ＳＴＢ）２については暗号化／復号化部（Ｄｅ－／Ｃｉｐｈｅｒ）が設けられている。

【００１３】コピープロテクトが必要なデジタルコンテンツはその送信側の機器によって暗号化された後にＩＥＥＥ１３９４シリアルバス１０上に出力され、その暗号化データは受信側の機器にて復号化されて暗号化が解除される。このようにＩＥＥＥ１３９４シリアルバス１０上に流れるデータを暗号化することにより、ＩＥＥＥ１３９４シリアルバス１０上に流れるデータが不正にコピーされてもそれが正常に再生されてしまうことを防止することができる。

【００１４】パーソナルコンピュータ（ＰＣ）１においては、暗号化／復号化部（Ｄｅ－／Ｃｉｐｈｅｒ）は、

図示のように、ＰＣＩバス２０などのシステムバスとＩＥＥＥ１３９４シリアルバス１０との間を双方向につなぐ１３９４ブリッジ６内に設けられる。これにより、ＰＣＩバス２０上には暗号化データは流れず、通常通り平文データだけが流れるので、オープンなバスアーキテクチャを維持できる。

【００１５】デジタルビデオカメラ（ＤＶＣ）３またはセットトップボックス（ＳＴＢ）２からＩＥＥＥ１３９４シリアルバス１０を介してパーソナルコンピュータ（ＰＣ）１に伝送される暗号化データは１３９４ブリッジ６によって平文に復号化された後、ＰＣＩバス２０上のＣＰＵ４やＭＰＥＧデコーダ５に送られる。同様に、ＣＰＵ４やＭＰＥＧデコーダ５からセットトップボックス（ＳＴＢ）２にデジタル映像コンテンツを送信するときは、ＰＣＩバス２０上の平文が１３９４ブリッジ６によって暗号化された後、ＩＥＥＥ１３９４シリアルバス１０上に送り出される。

【００１６】このように、１３９４ブリッジ６に暗号化／復号化機能を設けると、ＰＣＩバス２０のオープンアーキテクチャをそのまま維持することはできるが、ＰＣＩバス２０には暗号化が解かれたデータ（Ｐｌａｉｎ Ｃｏｎｔｅｎｔｓ）が流れてしまい容易にコピー可能となってしまう。

【００１７】また、１３９４ブリッジ６に暗号化／復号化機能を設けた図１５のパーソナルコンピュータにおいては、パーソナルコンピュータを構成する機能モジュール毎にその機能モジュールが扱うことができるコンテンツの種類（一回のみコピー可、コピー不可、コピーフリー）を制限するといった制御を行うことが困難となる。例えば、ＭＰＥＧ２デコーダについては全ての種類のコンテンツ（一回のみコピー可、コピー不可、コピーフリー）を扱えるようにする必要があるのに対し、ＤＶＤ－ＲＡＭやＨＤＤなどのストレージデバイスは一回のみコピー可のコンテンツとコピーフリーのコンテンツしか扱えことができないようにする事が必要となる。しかし、ＰＣＩバス２０にＰｌａｉｎ Ｃｏｎｔｅｎｔｓが流れてしまうと、機能モジュール毎にそれが扱うことができるコンテンツを制限することは実際上困難である。このようなコンテンツの制限は、通常、機器間の認証処理によって行われるからである。すなわち、１３９４ブリッジ６に暗号化／復号化機能を設けた場合には、パーソナルコンピュータもＩＥＥＥ１３９４シリアルバス上の一つの機器として扱われる。このため、パーソナルコンピュータとＩＥＥＥ１３９４シリアルバス上の他の機器との間の認証処理によって、そのパーソナルコンピュータが扱えるコンテンツの種類を制限することは可能ではあるが、パーソナルコンピュータ内の個々のモジュール単位でコンテンツの種類を制限することはできない。

【００１８】また、ＤＶＤビデオなどにおいては、デジタルコンテンツは、種類の異なる複数のコンテンツを含むストリームとして実現されている場合が多い。この場合、再生対象のコンテンツの種類がダイナミックに切り替わることになるが、コンテンツの種類が切り替わる度に認証をし直していたのでは、コンテンツをリアルタイムに処理することができなくなるという問題もある。

【００１９】本発明は上述の実情に鑑みてなされたものであり、パーソナルコンピュータなどのデータ処理装置内のバス上に流れるデジタルコンテンツの保護と、データ処理装置を構成する機能モジュール単位でのデジタルコンテンツの制限を実現できるようにし、デジタルコンテンツのコピープロテクトを効率よく行うことができるデータ処理装置および同装置に適用されるコピープロテクト方法を提供することを目的とする。

【００２０】

【課題を解決するための手段】上述の課題を解決するため、本発明は、コピープロテクト対象のデータを暗号化して授受するための認証機能を有する外部機器が接続可能な外部バスとのインターフェイスを有するデータ処理装置において、内部バスと、この内部バスにそれぞれ結合され、コピープロテクト対象のデータを前記内部バス経由で送信または受信する複数の機能モジュールと、前記各機能モジュール毎に設けられ、前記コピープロテクト対象のデータを授受する相手先の機能モジュールまたは前記外部機器との間で、前記コピープロテクト対象のデータを暗号化して授受するための認証処理を行う認証手段とを具備し、前記データ処理装置内の各機能モジュール毎に認証処理を行うことを特徴とする。

【００２１】このデータ処理装置においては、デジタルコンテンツなどのコピープロテクト対象のデータを扱う複数の機能モジュールそれぞれのインターフェイス部に認証手段が設けられており、機能モジュール間、あるいは機能モジュールと外部機器間で個別に認証処理が行われる。よって、それら機能モジュールが接続された内部バス上には、暗号化解除のためのキー、およびデジタルコンテンツは暗号化されたまま転送されるようになり、デジタルコンテンツの不正コピーを防止することができる。また、機能モジュール毎に認証処理を行っているので、機能モジュール単位でそれが扱うことが可能なデジタルコンテンツの種類（一回のみコピー可、コピー不可、コピーフリー）を効率よく制限することが可能となる。

【００２２】また、コピープロテクト対象のデータの暗号化／復号化機能を有する外部機器が接続可能な外部バスと前記データ処理装置内のバスとの間を透過的に接続する外部バスインターフェイス手段をさらに具備することにより、前記機能モジュール相互間、および前記外部機器と前記機能モジュールとの間の双方で、同一の認証および暗号化プロトコルを使用できるようにすることが可能となる。すなわち、データ処理装置内の各機能モジュールまたはアプリケーションプログラムから見ると、

データ処理装置内の機能モジュールと外部機器とを区別することなく、同様に扱うことが可能となる。

【００２３】また、前記コピープロテクト対象のデータの種類には一回のみコピー可のデータと、コピー不可のデータとがあり、前記各機能モジュールには、その機能モジュールが処理可能なデータの種類を規定するための識別情報が割り当てられており、前記認証手段は、送信対象のデータの種類と送信先の機能モジュールの識別情報（システムＩＤ）とに基づいて、前記送信先の機能モジュールが前記送信対象のデータを扱うことが可能な機能モジュールであるか否かを判別することが好ましい。

【００２４】このようにシステムＩＤを用いることにより、扱うことが可能なデジタルコンテンツの種類を機能モジュール単位で容易に管理することが可能となる。また、暗号化されたデータを復号化するために必要な暗号化解除キーは送信対象のデータの種類毎（一回のみコピー可、コピー不可）に変更することが好ましい。これにより、例えば認証処理時に各機能モジュールにそれが扱えるコンテンツに応じたキーのみを通知しておくことにより、複数の機能モジュールに暗号化コンテンツをブロードキャスト転送した場合であっても、そのコンテンツを扱える機能モジュールのみがその復号を行えるように制限することが可能となる。

【００２５】また、種類の異なる複数種のデータから構成されるストリームを送信するとき、前記認証手段は、送信先の機能モジュールが扱うことができるコンテンツの種類数だけ認証処理を行い、前記ストリームを構成するデータの種類の中で送信先の機能モジュールが処理可能なデータの種類数に対応する暗号化解除キーを前記送信先の機能モジュールに通知することが好ましい。このように受信側の機能モジュールに予めコンテンツの種類毎の暗号化解除キーを渡しておくことにより、コンテンツの種類がダイナミックに変更されても、リアルタイムに暗号化を解除することが可能となる。この場合、ストリームにはデータの種類を示すデータ種別情報を埋め込んでおき、復号化手段は、前記データ種別情報に基づいて、復号化処理に使用する暗号化解除キーを動的に変更すればよい。

【００２６】また、本発明は、内部バス上に流されるデジタルコンテンツの不正なコピーを防止するように受信装置側にデータを送信するデータ処理装置において、前記受信装置との間でコピープロテクト対象のデータの処理が許可されているか否かを認証する認証手段と、前記認証手段により認証された場合、前記受信装置が処理を許可されているコピープロテクト対象のデータが、どのような種類のデジタルコンテンツであるかを判別する判定手段と、この判定手段の判定結果に基づいて、前記受信装置が処理を許可されているデジタルコンテンツの種類にそれぞれ対応する暗号化解除キーを前記受信装置に送信するキー送信手段と、前記暗号化解除キーを利用して前記受信装置が暗号を解除できるデジタルコンテンツを送信する送信手段とを具備したことを特徴とする。

【００２７】このデータ処理装置においては、前記受信装置との間でコピープロテクト対象のデータの処理が許可されているか否かが認証され、認証された場合に、前記受信装置が処理を許可されているコピープロテクト対象のデータが、どのような種類のデジタルコンテンツであるかが判別され、そしてこの判定結果に基づいて、前記受信装置が処理を許可されているデジタルコンテンツの種類にそれぞれ対応する暗号化解除キーのみが前記受信装置に送信される。そして、この暗号化解除キーを利用して前記受信装置が暗号を解除できるデジタルコンテンツが受信装置に送信される。

【００２８】また、本発明は、内部バス上に流されるデジタルコンテンツの不正コピーを防止するように送信装置側から送信されたデータを受信処理するデータ処理装置において、前記送信装置との間でコピープロテクト対象のデータの処理が許可されているか否かを認証する認証手段と、前記認証手段により認証された場合、このデータ処理装置が処理を許可されているコピープロテクト対象のデジタルコンテンツの種類を示す情報を前記送信装置に送信する種類情報送信手段と、この種類情報に基づいて前記データ処理装置が処理を許可されているコピープロテクト対象のデジタルコンテンツの種類にそれぞれ対応する暗号化解除キーと、この暗号化解除キーを利用して前記データ処理装置が暗号を解除できるデジタルコンテンツとを、前記送信装置から受け取り、前記デジタルコンテンツを復号化する復号化手段とを具備したことを特徴とする。

【００２９】このデータ処理装置においては、前記送信装置との間でコピープロテクト対象のデータの処理が許可されているか否かが認証され、認証された場合、データの受信処理を許可されているコピープロテクト対象のデジタルコンテンツの種類を示す情報が前記送信装置に送信される。そして、種類情報に基づいて、前記受信処理を許可されているデジタルコンテンツの種類にそれぞれ対応する暗号化解除キーを前記送信装置より受け取り、次いでこの暗号化解除キーを利用して受信装置が暗号を解除できるデジタルコンテンツを前記送信装置から受け取る。そして前記デジタルコンテンツが前記暗号化解除キーを利用して復号化される。

【００３０】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。図１には、本発明の一実施形態に係るパーソナルコンピュータ（以下、ＰＣと称する）のシステム構成が示されている。このＰＣ１１は、ＩＥＥＥ１３９４シリアルバス２００を介して外部のコンシューマ電子機器、たとえば図示のようなセットトップボックス（ＳＴＢ）１２、デジタルビデオカメラまたはＤＶカムコーダ（ＤＶＣ）１３、およびデジタルビデオカセッ

トレコーダ（Ｄ－ＶＣＲ）１４と通信可能に構成されている。

【００３１】セットトップボックス（ＳＴＢ）１２、デジタルビデオカメラ（ＤＶＣ）１３、およびデジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）１４は、それぞれＩＥＥＥ１３９４コピープロテクト技術をサポートするために、ＩＥＥＥ１３９４シリアルバス２００とのインターフェイス部に、デバイス認証およびキー交換などを行う認証処理部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）１２１，１３１，１４１を有している。デジタルコンテンツの送受信を行うセットトップボックス（ＳＴＢ）１２およびデジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）１４については、暗号化・復号化双方の機能を持つ暗号化／復号化部（Ｄｅ－／Ｃｉｐｈｅｒ）１２２，１４２が設けられている。また、デジタルコンテンツの送信のみを行うデジタルビデオカメラ（ＤＶＣ）１３については、暗号化部（Ｃｉｐｈｅｒ）１３２だけが設けられている。

【００３２】ＰＣ１１、セットトップボックス（ＳＴＢ）１２、デジタルビデオカメラ（ＤＶＣ）１３、およびデジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）１４間で授受されるデジタルコンテンツは、暗号化された状態でＩＥＥＥ１３９４シリアルバス２００上を転送される。

【００３３】ＰＣ１１は、図示のように、ＰＣＩバス１００と、これに接続された複数の機能モジュールとから構成されている。これら機能モジュールの中で、デジタルコンタンツを扱う機能モジュール、つまり、ＣＰＵモジュール１１１、サテライトまたはデジタルＴＶ用のチューナ１１３、ＭＰＥＧ２デコーダ１１５、ＤＶＤ－ＲＡＭドライブ１１６については、ＰＣＩバス１００とのインターフェイス部に、機器認証およびキー交換などを行う認証処理部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）１１１，１１３１，１１５１，１１６１が設けられている。これら各認証処理部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）１１１１，１１３１，１１５１，１１６１の機能は、基本的に、１３９４デバイスであるセットトップボックス（ＳＴＢ）１２、デジタルビデオカメラ（ＤＶＣ）１３、およびデジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）１４のそれと同じであり、デジタルコンテンツを暗号化して授受するために必要な認証およびキー交換を行う。

【００３４】また、これらＣＰＵモジュール１１１、チューナ１１３、ＭＰＥＧ２デコーダ１１５のインターフェイス部には、さらに、暗号化されたコンテンツ（ｅｎｃｒｙｐｔｅｄ　ｃｏｎｔｅｎｔｓ）の暗号化を解除するための復号化処理を行う復号化部（Ｄｅ－ｃｉｐｈｅｒ）、または暗号化部（Ｃｉｐｈｅｒ）が設けられている。暗号化部を持つか復号化部を持つか、あるいはその両方を持つかは各機能モジュールの機能によって決まる。ここでは、チューナ１１３については暗号化部（Ｃｉｐｈｅｒ）１１３２が設けられ、ＣＰＵモジュール１１１およびＭＰＥＧ２デコーダ１１５については復号化部（Ｄｅ－ｃｉｐｈｅｒ）１１１２，１１５２が設けられている場合が例示されている。

【００３５】ＣＰＵモジュール１１１は、マイクロプロセッサと、メモリコントローラ、およびＰＣＩバスブリッジなどから構成されており、認証部１１１１と暗号解除部１１１２は例えばＰＣＩバスブリッジの一部として組み込むことができる。また、ＣＰＵモジュール１１１内の認証部１１１１、暗号解除部１１１２、ＭＰＥＧ２デコーダ部１１１３はソフトウェアで実現しても良い。

【００３６】ＤＶＤ－ＲＡＭドライブ１１６はＰＣ１１の補助記憶装置として設けられたものであり、ＩＤＥインターフェイスまたはＡＴＡＰＩインターフェイス等を介してＰＣＩバス１００に接続される。ＤＶＤ－ＲＡＭドライブ１１６は認証処理部１１６１のみを有し、復号化部（Ｄｅ－ｃｉｐｈｅｒ）、暗号化部（Ｃｉｐｈｅｒ）については設けられていない。暗号化されたデジタルコンテンツを暗号化した状態のままＤＶＤ－ＲＡＭ１１６に記録するためである。

【００３７】ＰＣ１１には、さらに、ＰＣＩバス１００とＩＥＥＥ１３９４シリアルバス２００間を双方向で接続する１３９４ブリッジ１１７が設けられている。１３９４ブリッジ１１７には、認証処理部、暗号化部、復号化部はどれも設けられておらず、暗号化されたデジタルコンテンツは暗号化された状態のままＰＣＩバス１００からＩＥＥＥ１３９４シリアルバス２００へ、またＩＥＥＥ１３９４シリアルバス２００からＰＣＩバス１００に転送される。このように、１３９４ブリッジ１１７は、ＰＣ１１内の機能モジュールと１３９４デバイスとの間を透過的に接続する。

【００３８】ここで、ＩＥＥＥ１３９４シリアルバス２００上のＤＶＣ１３から転送されるデジタルコンタンツを、ＣＰＵモジュール１１１でソフトウェアデコードする場合の処理手順について説明する。

【００３９】まず、ＤＶＣ１３とＣＰＵモジュール１１１との間で機器認証を行い、互いにコピープロテクト機能を有する正当なデバイスであることを確認し合う。この機器認証は、たとえば、ランダムチャレンジ＆レスポンス方法や、一方向関数を用いた方法、乱数を用いて毎回変わる時変キーを使用する方法、あるいはこれら方法の組み合わせなど、良く知られた方法を用いて実現できる。

【００４０】通信相手のデバイスがどのようなコンテンツの種類を扱うことができるものであるか否かの認証については、システムＩＤが用いられる。このシステムＩＤは、１３９４デバイスおよびＰＣ１１内の各機能モジュールの回路またはファームウェアなどに埋め込まれており、これによって、一回のみコピー可、コピー不可、

コピーフリーの全種類のデジタルコンテンツを扱えるデバイスであるか、一回のみコピー可あるいはコピーフリーのデジタルコンテンツだけを扱えるデバイスであるかが判別される。

【００４１】この認証処理にて、ＣＰＵモジュール１１１はＤＶＣ１３とキー交換を行い、暗号化されたコンテンツの暗号を解除するためのキーを生成する。認証部がＣＰＵモジュール１１１内にあるため、キー自身あるいはそれを生成するための情報は暗号化されたまま、１３９４バス２００およびＰＣＩバス１００を介してＤＶＣ１３からＣＰＵモジュール１１１に転送される。

【００４２】ＤＶＣ１３は、デジタルコンテンツを暗号化し、それをＣＰＵモジュール１１１に送る。暗号化されたコンテンツは暗号化されたまま１３９４バス２００およびＰＣＩバス１００を介してＣＰＵモジュール１１１に届き、ＣＰＵモジュール１１１の復号部（Ｄｅ－ｃｉｐｈｅｒ）１１１２は認証によって得たキーを使ってコンテンツの暗号を解く。ＣＰＵモジュール１１１の認証部と復号化部がソフトウェアによって実現されている場合には、このソフトウェアを改ざんできない、またはアルゴリズムが分からないような手だてを講じる必要があることはもちろんである。

【００４３】暗号を解かれたコンテンツはＣＰＵモジュール１１１内のソフトウェアＭＰＥＧ２デコーダ（Ｄｅｃｏｄｅｒ）１１１３によってデコードされた後、主メモリ１１２とＶＧＡコントローラ１１４を直接結ぶＡＧＰ（ＡｃｃｅｌｅｒａｔｅｄＧｒａｐｈｉｃｓ　Ｐｏｒｔ）を介してＶＧＡコントローラ１１４に送られて再生される。

【００４４】このように、デジタルコンテンツを扱う複数の機能モジュールそれぞれのインターフェイス部に認証処理部と、暗号化あるいは復号化部とを用意し、機能モジュール間あるいは機能モジュールと１３９４デバイス間でコピープロテクト対象のデジタルコンタンツを受け渡すときに、それらデバイス間で認証処理およびデジタルコンテンツの暗号化・復号化処理を行うことにより、ＩＥＥＥ１３９４バス２００およびＰＣＩバス１００のどちらにおいても暗号化解除のためのキー、およびデジタルコンテンツは暗号化されたまま転送されるようになり、デジタルコンテンツの不正コピーを防止することができる。

【００４５】また、ＰＣ１１内の各機能モジュール毎に認証処理を行うことができるので、機能モジュール単位で扱うことが可能なデジタルコンテンツの種類（一回のみコピー可、コピー不可、コピーフリー）を効率よく制限することが可能となる。

【００４６】図２には、図１のシステムにおけるソフトウェアとハードウェアとの関係が示されている。図２において、一点鎖線の上側がソフトウェア、下側がハードウェアである。また、縦方向に階層化されて示されている太枠のブロックがＰＣ１１内の各機能モジュールまたは１３９４デバイスなどのハードウェアデバイスである。

【００４７】Ａｕｔｈｅｎｔｉｃａｔｏｒハンドラは、デジタルコンテンツ再生用ソフトなどのアプリケーションプログラムからの要求に応じて、必要な各ハードウェアデバイスとの間で認証処理やキー交換のための制御を行う。前述したように、１３９４ブリッジ１１７はＰＣ１１内の各機能モジュールと１３９４デバイスとを透過的に接続するので、ＰＣ１１内の各機能モジュールに１３９４デバイスと同様の認証および暗号化／復号化プロトコルを実装することにより、点線で示されているように、アプリケーションプログラムからはＰＣ１１内の各機能モジュールと１３９４デバイスとを区別することなくそれらを等価に扱うことが可能となる。

【００４８】図３には、本実施形態で用いられる認証処理およびキー交換の手順の一例が示されている。コンテンツを送信する側のデバイスがＳｏｕｒｃｅ　Ｄｅｖｉｃｅ、受信する側のデバイスがＳｉｎｋ　Ｄｅｖｉｃｅである。

【００４９】Ｓｉｎｋ　Ｄｅｖｉｃｅは、まず、乱数を使って毎回変わる代わるランダムチャレンジキー（Ｎａ）を生成し、認証要求と共にそのランダムチャレンジキー（Ｎａ）を、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅに渡す。そして、Ｓｉｎｋ　Ｄｅｖｉｃｅは、決められた関数を用いてＮａからＡｒを作成する。

【００５０】Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、乱数を使って毎回変わる代わるランダムチャレンジキー（Ｎｂ）を生成し、それを、認証要求に対する応答としてＳｉｎｋＤｅｖｉｃｅに返す。そして、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、決められた関数を用いてＮｂからＢｒを作成する。

【００５１】この後、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、メッセージ（Ｂｖ）をＳｉｎｋ　Ｄｅｖｉｃｅに送る。このメッセージ（Ｂｖ）は、公開鍵と、Ｎａ，Ｂｒとから作成されたものである。

【００５２】Ｓｉｎｋ　Ｄｅｖｉｃｅは、メッセージ（Ａｖ）をＳｏｕｒｃｅ　Ｄｅｖｉｃｅに送る。メッセージ（Ａｖ）は、公開鍵と、Ｎｂ，Ａｒとから作成されたものである。

【００５３】Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、Ａｖが正しいか確認し、正しければ相手が正当なデバイスであると判断して認証鍵（Ａｋ）を作る。同様に、Ｓｉｎｋ　Ｄｅｖｉｃｅも、Ｂｖが正しいか確認し、正しければ相手が正当なデバイスであると判断して認証鍵（Ａｋ）を作る。

【００５４】この後、Ｓｏｕｒｃｅ　Ｄｅｖｉｃｅは、認証鍵（Ａｋ）で暗号化したコントロール鍵（ｅＫｘ）をＳｉｎｋ　Ｄｅｖｉｃｅに送る。Ｓｉｎｋ　Ｄｅｖｉｃｅは、暗号化されたコントロール鍵（ｅＫｘ）を認証

鍵（Ａｋ）で暗号を解除し、コントロール鍵（Ｋｘ）を作る。

【００５５】なお、図３の認証処理の手順はあくまで一例であり、互いのデバイスが互いに正しいデバイスであることを検証し合うことができるものであれば、前述したように、通常のランダムチャレンジ＆レスポンス方法や、その他の良く知られた方法を利用することができる。

【００５６】次に、転送されるデジタルコンテンツの種類（１回コピー可、コピー不可、コピーフリー）がリアルタイムに切り替わる場合において、扱うことが可能なコンテンツを各デバイス毎に制限する方法について説明する。

【００５７】コピー不可、１回のみコピー可のコンテンツを送信可能なデバイスは、コピー不可用と１回のみコピー可用の２種類のコントロールキー（コンテンツ暗号解除キーの暗号化を解くキー）を別々に用意し、受信側のデバイスの能力に応じて、それに渡すコントロールキーの数を変更する。また、受信側のデバイスが両方の（コピー不可、１回のみコピー可）コンテンツを扱える場合は２回認証を行い、両方のコントロールキーを予め取得する。送信側のデバイスにおいて、コンテンツの種類に応じてキーを変更するのは当然のことだが、認証処理によってあらかじめ両方のキーを受信側に準備させておくことにより、コンテンツの種類のダイナミックな切り替えに柔軟に対応することができる。

【００５８】以下、この認証処理の具体的な手順の一例を図４のフローチャートを参照して説明する。まず、デジタルコンテンツの送信先となる受信側の各デバイス毎に、以下の処理が行われる。まず、受信側のデバイスからシステムＩＤを取得する。そして、そのシステムＩＤに基づいて、その受信側デバイスがコピー不可コンテンツを扱うことができるか否かを判断する（ステップＳ１０１）。受信側デバイスがコピー不可コンテンツを扱うことができるデバイスであれば、送信側デバイスから受信側デバイスに対してコピー不可コンテンツ用のコントロールキー（ｅＫｃｏｎｔｒｏｌ＃１）を送信し、受信側デバイスはそのコピー不可コンテンツ用のコントロールキー（ｅＫｃｏｎｔｒｏｌ＃１）を受け取る（ステップＳ１０２）。コピー不可コンテンツを扱うことができないデバイスに対しては、コピー不可コンテンツ用のコントロールキーの送信は行われない。

【００５９】次に、システムＩＤに基づいて、その受信側デバイスが１回のみコピー可のコンテンツを扱うことができるか否かを判断する（ステップＳ１０３）。受信側デバイスが１回のみコピー可のコンテンツを扱うことができるデバイスであれば、送信側デバイスから受信側デバイスに対して１回のみコピー可コンテンツ用のコントロールキー（ｅＫｃｏｎｔｒｏｌ＃２）を送信し、受信側デバイスはそのコントロールキー（ｅＫｃｏｎｔｒｏｌ＃２）を受け取る（ステップＳ１０４）。１回のみコピー可コンテンツを扱えないデバイスに対しては、１回のみコピー可コンテンツ用のコントロールキーの送信は行われない。

【００６０】これら各コントロールキー（ｅＫｃｏｎｔｒｏｌ＃１，＃２）は前述したように暗号化されたコンテンツキーの暗号化を解除するためのキーを暗号化したものであり、乱数などを用いた時変キーを用いることができる。受信側のデバイスでは、認証処理で授受される乱数値や予めデバイス内に用意されている他のキーを用いてｅＫｃｏｎｔｒｏｌ＃１，＃２の暗号化を解き、Ｋｃｏｎｔｒｏｌ＃１，＃２が得られる。

【００６１】このようにして、各受信側デバイス毎にそのデバイスの機能に応じたキーが渡される。すなわち、コピー不可、１回のみコピー可の両方のコンテンツを扱えるデバイスの場合は２回の認証によって両方のコントロールキーが渡される。また、１回のみコピー可のコンテンツのみを扱えるデバイスの場合には、１回のみコピー可コンテンツ用のコントロールキーのみが渡されることになる。

【００６２】全ての受信側デバイスとの認証処理が終了すると（ステップＳ１０５）、暗号化されたコンテンツキー（ｅＫｃｏｎｔｅｎｔ）と、暗号化されたコンテンツ（Ｅｎｃｒｙｐｔｅｄ　ｃｏｎｔｅｎｔｓ）とが、送信側デバイスから全ての受信側デバイスにブロードキャスト送信される（ステップＳ１０６，Ｓ１０７）。暗号化されたコンテンツ（Ｅｎｃｒｙｐｔｅｄ　ｃｏｎｔｅｎｔｓ）のヘッダ部には、コピー不可、１回のみコピー可、コピーフリーのいずれかを示すコピーコントロール情報（ＣＧＭＳ）が埋め込まれている。

【００６３】受信側の各デバイスは、コピーコントロール情報（ＣＧＭＳ）を、コントロールキーを動的に変更するためのコンテンツ識別情報として使用する。すなわち、受信側の各デバイスは、暗号化されたコンテンツに含まれるコピーコントロール情報（ＣＧＭＳ）に従って現在受信処理中のコンテンツの種類を判別し、そのコンテンツの種類に対応したコントロールキー（Ｋｃｏｎｔｒｏｌ）を選択する。そして、その選択したコントロールキーを用いることによって、暗号化されたコンテンツキー（ｅＫｃｏｎｔｅｎｔ）の暗号化を解除し、暗号化されたコンテンツ（Ｅｎｃｒｙｐｔｅｄ　ｃｏｎｔｅｎｔｓ）の暗号化を解除するためのコンテンツキー（Ｋｃｏｎｔｅｎｔ）を生成する（ステップＳ１０８）。扱えない種類のコンテンツを受信した受信側のデバイスについては、対応するコントロールキー（Ｋｃｏｎｔｒｏｌ）が無いのでそのコンテンツの暗号化を解除することは出来ない。

【００６４】このように、本実施形態では、種類の異なる複数種のコンテンツから構成されるストリームを送信するときは、受信側のデバイスが扱うことができるコン

テンツの種類数だけ認証処理を行い、ストリームを構成するコンテンツの種類の中で受信側のデバイスが処理可能なコンテンツの種類数に対応する暗号化解除用のキーをその受信側のデバイスに渡すという処理が行われる。

【００６５】ここで、例えば図５のように、一回のみコピー可のコンテンツからなる暗号化サブストリームＡとコピー不可のコンテンツからなる暗号化サブストリームＢとを連続して送信する場合を想定する。

【００６６】各暗号化サブストリームＡ，Ｂの各々のヘッダ部には、図６に示すように、使用するキーの変更を指示するための情報として、コンテンの種類を示すコンテンツ識別情報が埋め込まれている。このコンテンツ識別情報としては、前述したようにコピーコントロール情報（ＣＧＭＳ）を使用することができる。

【００６７】このような暗号化ストリームを、コピー不可、１回のみコピー可の両方のコンテンツを扱えるデバイス（デバイス＃１）と、１回のみコピー可のコンテンツもしくはコピーフリーのコンテンツのみを扱えるデバイス（デバイス＃２）に送信する場合には、デバイス＃１については暗号化サブストリームＡ，Ｂ双方の暗号化解除キーが渡され、デバイス＃２については暗号化サブストリームＢの暗号化解除キーだけが渡されることになる。

【００６８】したがって、図７（ａ）に示されているように、デバイス＃１は、暗号化サブストリームＡから暗号化サブストリームＢにコンテンツの種類が切り替わった時に、それに応じて暗号化解除キーを動的に変更することにより、暗号化サブストリームＡ，Ｂそれぞれに対応する正しい復号データ（平文）を得ることができる。一方、図７（ｂ）に示されているように、デバイス＃２は、暗号化サブストリームＢの暗号化を解除するためのキーを有してないので、暗号化サブストリームＡに対応する復号データ（平文）を得ることは出来るが、暗号化サブストリームＢについてはその暗号化を解除することはできない。

【００６９】なお、ここでは、各受信側デバイス毎にそのデバイスの機能に応じたコントロールキーを渡すようにしたが、各受信側デバイス毎にそのデバイスの機能に応じたコンテンツキーを準備させることが肝要であるので、そのための手順としては使用する認証処理の方法により様々な手法を用いることができる。また、各機能モジュール毎に認証部や暗号化／復号化部を設ける構成は、ＰＣのみならず、例えば、デジタルコンテンツの録画／再生用プレーヤなどの各種マイクロコンピュータ応用装置に適用することができる。

【００７０】次に、図８を参照して、図１のＰＣ１１においてコンテンツをストレージデバイスに記録する方法について説明する。一般に、パーソナルコンピュータにおいて補助記憶装置として用いられるストレージデバイスには認証機能が設けられてないため、コピープロテクトが必要なコンテンツを記録することはできない。また、認証機能と復号化機能を用意すればコンテンツの暗号化を解除した後にストレージデバイスに記録することが可能となるが、このようにすると、今度は、その記録内容（Ｐｌａｉｎ　Ｃｏｎｔｅｎｔｓ）が不正に使用されてしまう危険がある。特に、可搬型の記録メディアを使用するリムーバブルストレージデバイスの場合には、その危険が高い。

【００７１】そこで、本実施形態では、ストレージデバイスには認証処理部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）のみを設け、コンテンツを暗号化したまま記録メディアに記録すると共に、さらに認証によって生成されたコンテンツキーを、システムがアクセスできない記録メディア上の領域に記録するようにしている。

【００７２】以下、コピープロテクトが必要な一回のみコピー可のデジタルコンテンツをＳＴＢ１２から受信してＤＶＤ－ＲＡＭドライブ１１６のＤＶＤ－ＲＡＭメディアに記録する場合を例示してその記録方法について具体的に説明する。

【００７３】１．ＳＴＢ１２とＤＶＤ－ＲＡＭドライブ１１６それぞれの認証部（Ａｕｔｈｎｔｉｃａｔｏｒ）１２１，１１６１を使って、それらデバイス間の認証を行い、互いに正当なデバイスであることが確認されると、ＳＴＢ１２側から暗号化されて送られて来るコントロールキー（ｅＫｃｏｎｔｒｏｌ）をＤＶＤ－ＲＡＭドライブ１１６側で暗号を解きコントロールキー（Ｋｃｏｎｔｒｏｌ）を生成する。

【００７４】２．ＳＴＢ１２から暗号化されたコンテンツキー（ｅｋｃｏｎｔｅｎｔ）が暗号化されたデジタルコンテンツと共にＤＶＤ－ＲＡＭドライブ１１６に送られる。

【００７５】３．暗号化されたデジタルコンテンツにはコピーコントロール情報（ＣＧＭＳ）が含まれている。４．ＤＶＤ－ＲＡＭドライブ１１６はＫｃｏｎｔｒｏｌとＣＧＭＳを使ってｅＫｃｏｎｔｅｎｔからコンテンツキー（Ｋｃｏｎｔｅｎｔ）を生成する。ｅＫｃｏｎｔｅｎｔは時変キーである。

【００７６】５．Ｋｃｏｎｔｅｎｔで暗号化された暗号化コンテンツ（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔｓ）はそのままメディアの上に記録され、対応するＫｃｏｎｔｅｎｔは例えば図９のようにセクター間のギャップ領域に記録される。またＣＧＭＳの内容は“１回コピー可能”から“これ以上コピー不可”の状態に変更され、同様にこのギャップ領域に記録する。このギャップ領域はシステムからはアクセスできない領域である。

【００７７】なお、これら手順のコントロールはすべてＣＰＵモジュール１１１によって行われる。次に、図１０を参照して、ＤＶＤ－ＲＡＭメディアに記録された暗号化コンテンツ（ＥｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔｓ）を再生する場合について説明する。

【００７８】１．ＤＶＤ－ＲＡＭドライブ１１６とＭＰＥＧ２デコーダ１１５との間で、認証を行う。
２．互いに正当なデバイスであることが確認されると、暗号化されたコントロールキー（ｅＫｃｏｎｔｒｏｌ）がＤＶＤ－ＲＡＭドライブ１１６からＭＰＥＧ２デコーダ１１５に送られる。
【００７９】３．ＭＰＥＧ２デコーダ１１５内のＡｕｔｈｅｎｔｉｃａｔｏｒ１１５１でｅＫｃｏｎｔｒｏｌの暗号化を解き、Ｋｃｏｎｔｒｏｌが作られる。
４．暗号化コンテンツ（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔｓ）と同時に暗号化されたコンテンツキー（ｅｋｃｏｎｔｅｎｔ）とＣＧＭＳがＤＶＤ－ＲＡＭドライブ１１６からＭＰＥＧ２デコーダ１１５へ送られる。
【００８０】５．ＭＰＥＧ２デコーダ１１５のＡｕｔｈｅｎｔｉｃａｔｏｒ１１５１でＫｃｏｎｔｒｏｌとＣＧＭＳからｅＫｃｏｎｔｅｎｔの暗号化を解きＫｃｏｎｔｅｎｔを生成する。
【００８１】６．ＭＰＥＧ２デコーダ１１５内のＤｅ－Ｃｉｐｈｅｒ１１５２にＫｃｏｎｔｅｎｔを送る。
７．Ｄｅ－Ｃｉｐｈｅｒ１１５２はコンテンツキーにより暗号化コンテンツ（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔｓ）の暗号化を解き、そのコンテンツのＰｌａｉｎ　Ｔｅｘｔを生成する。
【００８２】８．ＭＰＥＧ２デコーダ１１５はＰｌａｉｎＴｘｅｔをデコードした後にＶＧＡコントローラ１１４のビデオ入力ポートに送り、それを画面表示する。以上のように、ストレージデバイスのバスインターフェース部に機器認証用のＡｕｔｈｅｎｔｉｃａｔｏｒ部を設け、送られて来た暗号化コンテンツをそのまま記録することにより、今まで、記録できなかった１回コピー可能なコンテンツをストレージデバイスに記録できるようになる。また、送られて来たコンテンツをそのまま記録することにより、コンテンツ暗号解除のための復号化回路が不要になる。また、暗号化解除されたコンテンツ暗号解除キーを、システムから読み出せない領域に書き込むことにより、正当なデバイスだけが、ストレージデバイスとの認証によってそのストレージデバイスの記憶内容の暗号化解除を行うことが可能となる。
【００８３】また、このように暗号化されたデジタルコンテンツが通常の領域に記録され、その暗号化解除のためのキーがシステムからは読み出しできない領域に記録されるコンピュータ読み取り可能な記録媒体を用いて各種タイトルを配布するようにしてもよい。これにより、認証および暗号化／復号化機能を持つ正当な機器でしかその記録媒体の内容を再生できなくなり、不正コピーを防止することが可能となる。
【００８４】なお、ここでは、ストレージデバイスとしてＤＶＤ－ＲＡＭドライブを例示したが、ＤＶＤ－Ｒドライブ、ＭＯドライブ、ＨＤＤなどに適用しても良い。また、このように認証機能を有するストレージデバイスはＰＣのみならず、例えばＤＶＤプレーヤとＤ－ＶＣＲの複合機など、リード／ライト可能なストレージデバイスを使用する各種マイクロコンピュータ応用装置に適用することができる。また、ＩＥＥＥ１３９４デバイスとして実現してもよいことはもちろんである。
【００８５】次に、暗号化して転送されるコンテンツの属性（分野、地域）を用いて、そのコンテンツを扱うことができるデバイスを制限するというデータ転送制限方法について説明する。
【００８６】すなわち、これまでは、コピー不可、一回のみコピー化、コピーフリーというコピー制御情報に基づいてそれを扱うことができるデバイスを制限する方法について説明したが、この方法は、基本的には、同一種類のコンテンツからなるストリーム全体を単位とした制御である。したがって、扱うことが許された種類のコンテンツの中で、ある特定の条件に適合した部分だけを扱えるようにするといったきめ細かな制御を行うことは困難である。
【００８７】そこで、本データ転送制限方法では、ストリームデータのヘッダ部にコンテンツの内容を示す分野情報や地域情報を埋め込み、それら分野情報や地域情報を用いることにより、扱うことが許された種類（コピー不可、一回のみコピー化、またはコピーフリー）のコンテンツからなるストリームの中で、ユーザ等によって予め指定された条件（分野、地域）に適合する部分のみを処理可能にし、それ以外の他の部分については処理できないようにしている。
【００８８】図１１には、本データ転送制限方法を実現するためのシステム構成が示されている。まず、ストリームデータのバケットヘッダ部に付加された分野情報に応じた転送制御について説明する。
【００８９】ここでいう、「分野」とは性的描写の有無・程度、暴力的描写の有無・程度、などの社会的、教育的に要請される分類を意味する。ストリームデータはネットワーク経路の通過時点でパケット化され、このパケットはデータの情報を持つヘッダ部とデータそのものから構成される。なお、ここでいうヘッダ部とはネットワーク経路が規定するヘッダであっても、データが内包するヘッダ部分であってもかまわない。
【００９０】データ出力システム３０１はストリームデータの記憶装置３０２とそれを外部に出力するインタフェース部３０３とから構成される。ここで、ネットワーク経路に出力すべきデータパケットを作成する。「分野」の情報は、図１２のようにそのパケットのヘッダ部に格納される。ネットワークは有線・無線の別を問わない。また、図１のＩＥＥＥ１３９４シリアルバス２００やＰＣＩバス１００などであってもよい。
【００９１】データ処理システム４０１はストリームデータを受け取る装置内にある。例えば、図１のＰＣ１１においては、チューナ１１３、ＣＰＵモジュール１１

１、あるいはＭＰＥＧ２デコーダ１１５などがデータ処理システム４０１に相当することになる。また、データ処理システム４０１はＰＣのみならず、図の１３９４デバイスであってよく、またサテライト端末やインターネット端末であってもよい。

【００９２】データ処理システム４０１は実際にデータをユーザに提示するための処理を行う部分で、データを受け取るインタフェース部４０２と処理を行うストリームデータ処理部４０３とから構成される。すなわち、「分野」情報はデータを受信した時点ではなくデータ自身を処理するタイミングで解読され、データ処理システム４０１のユーザ等によって予め設定されたシステム属性情報で定義される分野、との比較によってそのデータの処理の可否がデータパケット単位で決定される。

【００９３】なお、インタフェース部はソフトウェアのみ、ハードウェアのみ、両者の結合体のいずれでもよい。また、ストリームデータには「分野」情報のみならず、その代わりに、あるいはそれに追加して、対応するコンテンツを処理可能な地域を特定するための「地域」情報を埋め込むようにしても良い。ここで、「地域」とはストリームデータの作成者、または配信者の意図に応じて分類されたものである。この場合にも、「地域」情報はデータを受信した時点ではなくデータ自身を処理するタイミングで解読され、データ処理システム４０１のシステム情報で規定された地域との比較によってそのデータの処理の可否がデータパケット単位で決定される。

【００９４】図１３には、ストリームのパケットヘッダに埋め込まれた「分野」、「地域」などのストリーム属性情報によってデータの処理の可否を制御する様子が示されている。

【００９５】図１３においては、データ処理システム４０１が扱うことが可能な種類のデジタルコンテンツがデータパケットＡ，Ｂ，Ｃ，Ｄから構成されており、各データパケット毎にそのヘッダ部に「分野」または「地域」情報がストリーム属性情報として含まれている場合が示されている。

【００９６】データ処理システム４０１のストリーム制限機能により、データ処理システム４０１に適合する「分野」または「地域」のデータ（データＡ，データＣ）だけが処理され、他のデータ（データＢ，データＤ）は処理対象から除外され廃棄される。ストリーム制限機能の処理は、図１４のフローチャートに示す手順によって実行される。すなわち、まず、データ処理システム４０１に設定されているシステム属性情報が取得され、受信したストリームのパケットヘッダに含まれているストリーム属性情報との比較が行われる（ステップＳ２０１～Ｓ２０４）。一致しているならば、そのストリーム（パケット）の処理が行われ（ステップＳ２０５）、不一致ならば処理されない（ステップＳ２０６）。

【００９７】したがって、例えば、図１のＭＰＥＧ２デコーダ１１５にデータ処理システム４０１のストリーム制限機能を付加した場合には、連続して転送される映像コンテンツ（データＡ，Ｂ，Ｃ，Ｄ）の中で、ユーザ設定の「分野」または「地域」に合致するデータ（データＡ，データＣ）だけがデコードおよび再生され、他のデータ（データＢ，データＤ）についてはそのデコードおよび再生が行われない。つまり、データＡが再生された後、データＢの再生期間はブランキングとなり、データＢの再生期間が終わるとデータＣが再生されることになる。

【００９８】よって、図１１のシステム構成をサテライトＴＶ放送などのように不特定多数を相手とするコンテンツ提供システムに適用することにより、各ユーザの条件に合致したシーンだけを再生したり、記録することが可能となり、扱うことが許された種類のコンテンツの中で、ある特定の条件に適合した部分だけを扱えるようにするといったきめ細かな制御を容易に実現できるようになる。

【００９９】

【発明の効果】以上説明したように、本発明によれば、パーソナルコンピュータなどのデータ処理装置を構成する機能モジュールそれぞれに暗号化処理のための認証機能を設けることにより、機能モジュール間を接続するバス上に流れるデジタルコンテンツの保護と、機能モジュール単位でのデジタルコンテンツの制限を効率よく実現できるようになる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るコンピュータシステムのシステム構成を示すブロック図。

【図２】図１のシステムにおけるソフトウェアとハードウェアとの関係を示す図。

【図３】図１のシステムで用いられる機器認証およびキー交換の一例を示す図。

【図４】同実施形態のシステムで使用される認証処理の具体的な手順の一例を示すフローチャート。

【図５】同実施形態のシステムに適用されるデジタルコンテンツのストリーム構成の一例を示す図。

【図６】同実施形態のシステムに適用されるデジタルコンテンツのパケットヘッダにコンテンツ識別情報を付加した様子を示す図。

【図７】同実施形態のシステムに適用されるデジタルコンテンツ制限処理の原理を説明するための図。

【図８】同実施形態のシステムに設けられたストレージデバイスへのコンテンツ記録動作を説明するための図。

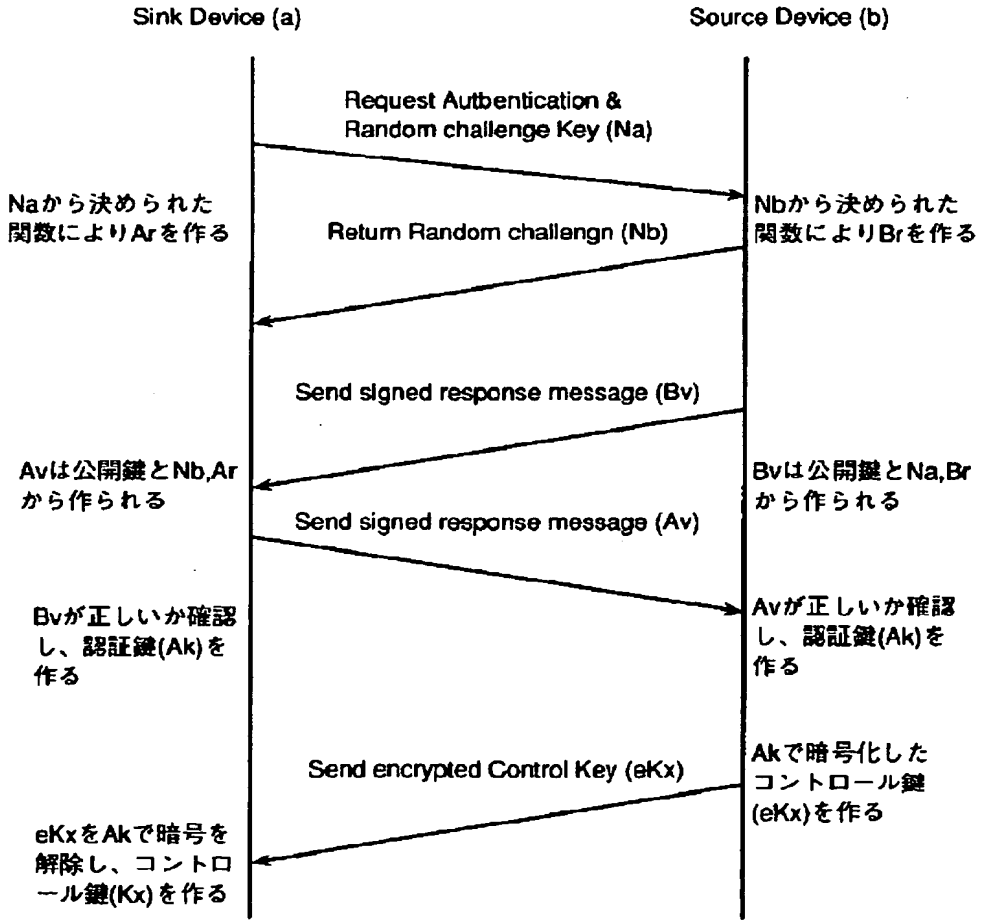
【図９】同実施形態のシステムに設けられたストレージデバイスにおけるキーの記憶方式を説明するための図。

【図１０】同実施形態のシステムに設けられたストレージデバイスに記録されているコンテンツの再生動作を説明するための図。

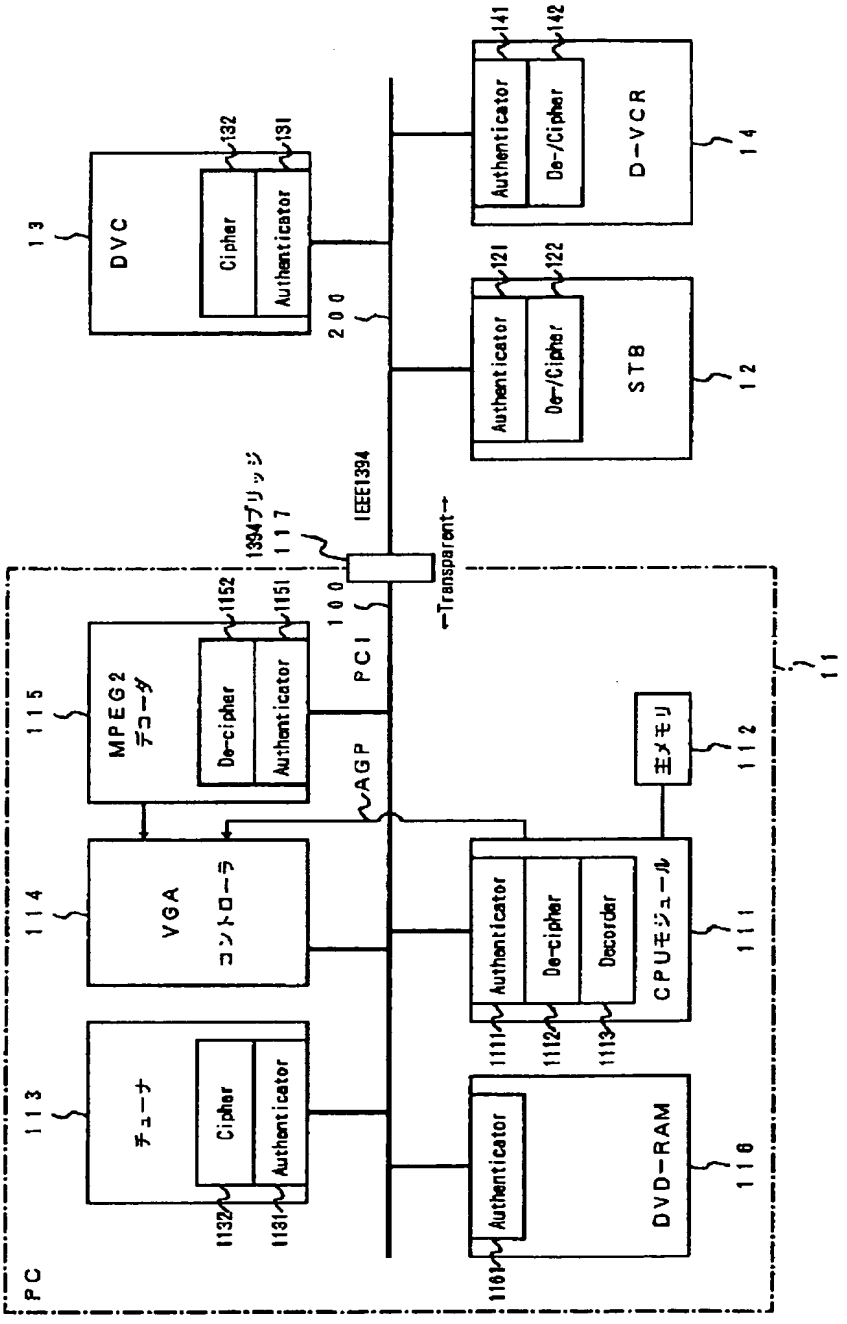
【図１１】同実施形態のシステムに適用されるデータ転送制限方法の原理を説明するための図。
【図１２】図１１のデータ転送制限方法で使用されるストリームデータの構造の一例を示す図。
【図１３】図１１のデータ転送制限方法によるデータ制限処理動作を示す図。
【図１４】図１１のデータ転送制限方法の処理手順を示すフローチャート。
【図１５】１３９４ブリッジに暗号化／復号化機能を設けたコンピュータシステムのシステム構成を示すブロック図。
【符号の説明】
１１…パーソナルコンピュータ（ＰＣ）
１２…セットトップボックス（ＳＴＢ）
１３…デジタルビデオカメラまたはＤＶカムコーダ（ＤＶＣ）
１４…デジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）
１１１…ＣＰＵモジュール
１１２…主メモリ
＊１１３…サイライトまたはデジタルＴＶチューナ
１１４…ＶＧＡコントローラ
１１５…ＭＰＥＧ２デコーダ
１１６…ＤＶＤ－ＲＡＭドライブ
１１７…１３９４ブリッジ
１２１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１２２…暗号化・復号化部（Ｄｅ－／Ｃｉｐｈｅｒ）
１３１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１３２…暗号化部（Ｃｉｐｈｅｒ）
１４１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１４２…暗号化・復号化部（Ｄｅ－／Ｃｉｐｈｅｒ）
１１１１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１１１２…復号化部（Ｄｅ－ｃｉｐｈｅｒ）
１１３１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１１３２…暗号化部（Ｃｉｐｈｅｒ）
１１５１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）
１１５２…復号化部（Ｄｅ－ｃｉｐｈｅｒ）
１１６１…認証部（Ａｕｔｈｅｎｔｉｃａｔｏｒ）

＊

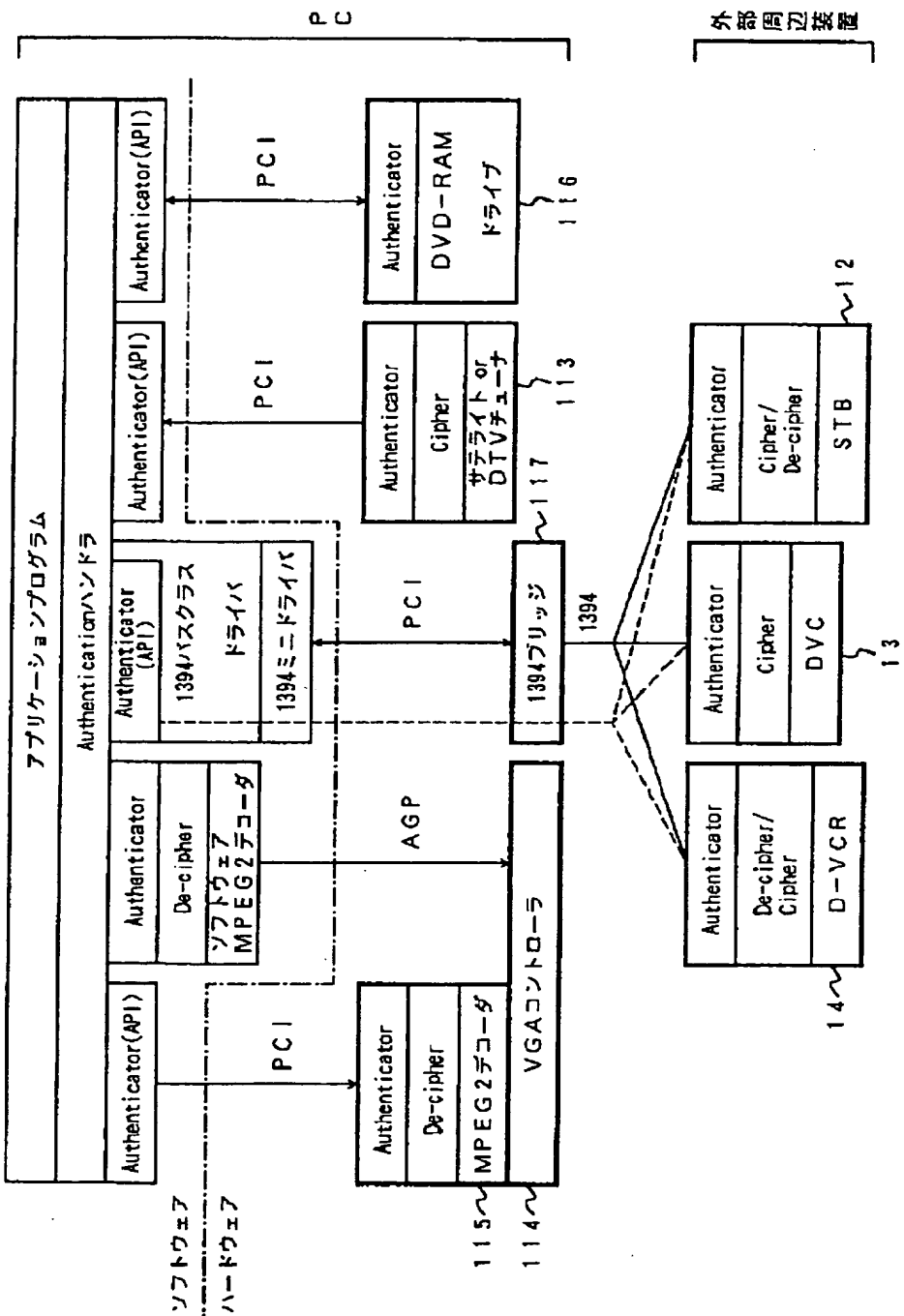
【図３】



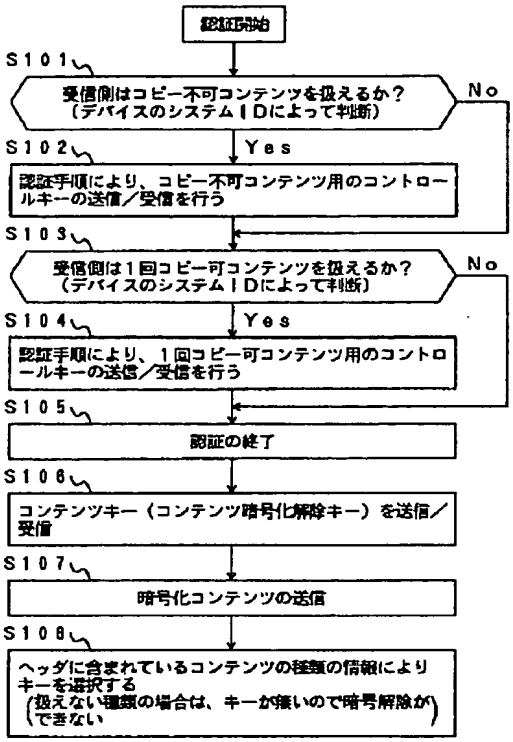
【図１】


PC
11
CPUモジュール
111
Authenticator
De-cipher
Decorder
1111
1112
1113
主メモリ
112
VGA
コントローラ
114
MPEG2
デコーダ
115
De-cipher
Authenticator
1152
1151
PCI
100
AGP
1394ブリッジ
117
IEEE1394
←Transparent→
DVD-RAM
116
1101
チューナ
113
Cipher
Authenticator
1132
1131
DVC
13
132
131
200
D-VCR
14
141
142
STB
12
121
122

【図２】

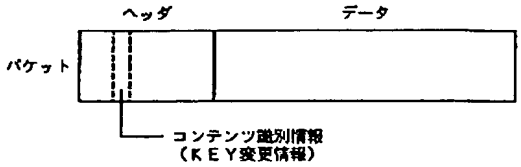

PC
外部周辺装置
アプリケーションプログラム
Authentication ハンドラ
Authenticator(API)
Authenticator
De-cipher
ソフトウェア MPEG2デコーダ
1394バスクラス ドライバ
1394ミニドライバ
1394ブリッジ
1394
PCI
AGP
Authenticator
Cipher
サテライト or DTVチューナ
Authenticator
DVD-RAM ドライブ
Authenticator
Cipher/ De-cipher
STB
Authenticator
Cipher
DVC
Authenticator
De-cipher/ Cipher
D-VCR
Authenticator
De-cipher
MPEG2デコーダ
VGAコントローラ
ソフトウェア
ハードウェア
115
114
117
113
116
12
13
14

【図４】

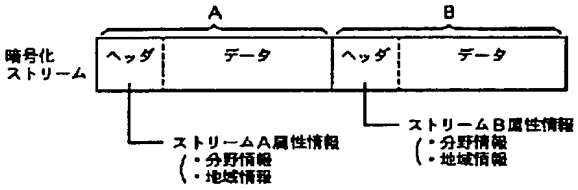


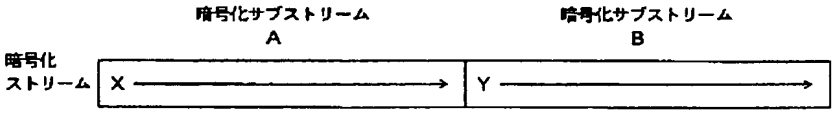
【図５】

【図６】



【図１２】

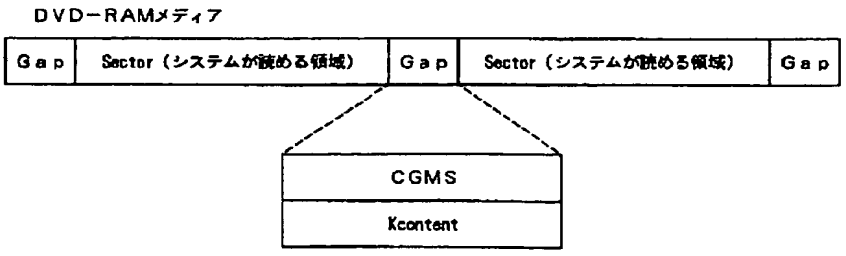




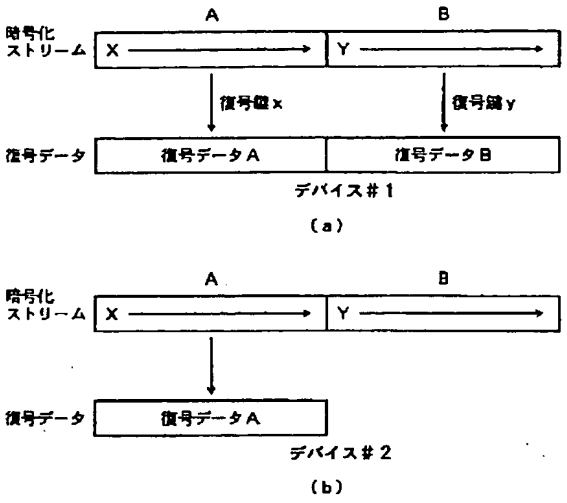
サブストリームＡ：１回のみコピー可／暗号鍵X

サブストリームＢ：コピー不可／暗号鍵Y

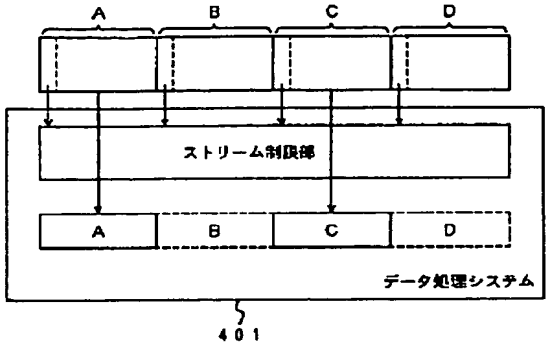
【図９】



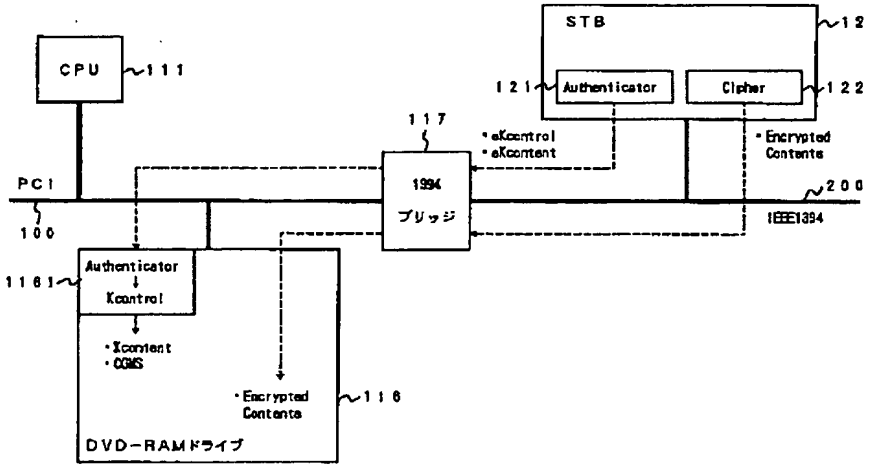
【図７】


暗号化ストリーム
A
B
X
Y
復号鍵x
復号鍵y
復号データ
復号データA
復号データB
デバイス＃１
(a)
暗号化ストリーム
A
B
X
Y
復号データ
復号データA
デバイス＃２
(b)

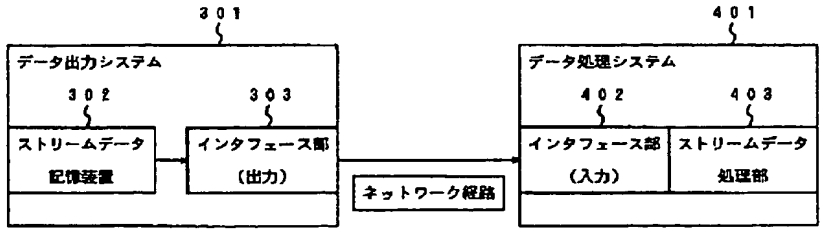
【図１３】


A
B
C
D
ストリーム制限部
A
B
C
D
データ処理システム
４０１

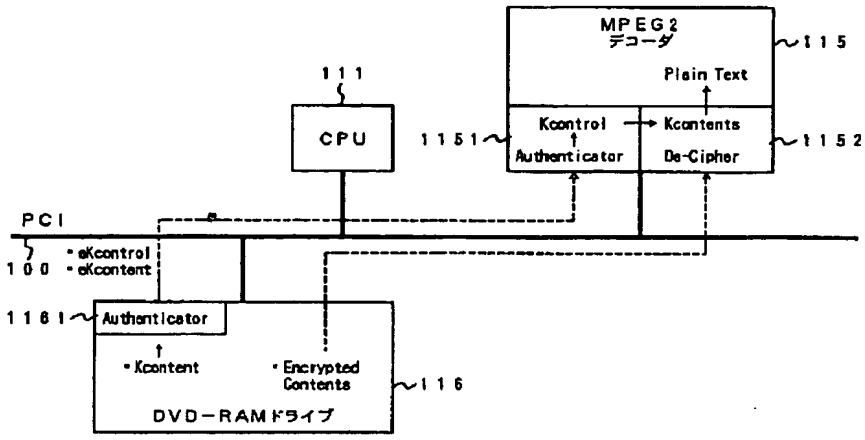
【図８】


CPU
１１１
STB
１２
１２１
Authenticator
Cipher
１２２
１１７
・eKcontrol
・eKcontent
・Encrypted Contents
PCI
１００
1394 ブリッジ
２００
IEEE1394
Authenticator
↓
Kcontrol
１１８１
・Kcontent
・CCMS
・Encrypted Contents
１１６
DVD－RAMドライブ

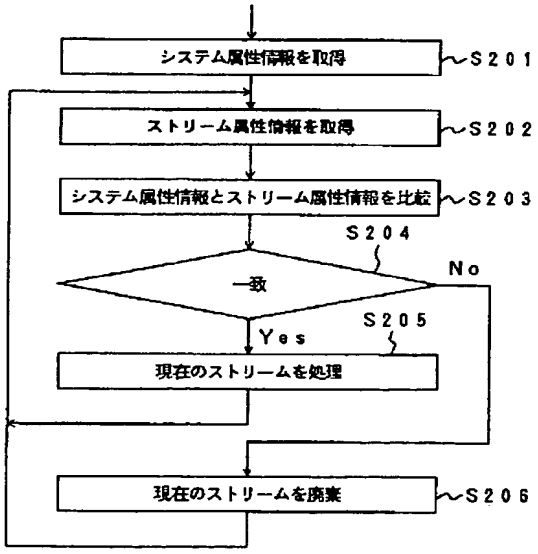
【図１１】


３０１
データ出力システム
３０２
３０３
ストリームデータ記憶装置
インタフェース部（出力）
ネットワーク経路
４０１
データ処理システム
４０２
４０３
インタフェース部（入力）
ストリームデータ処理部

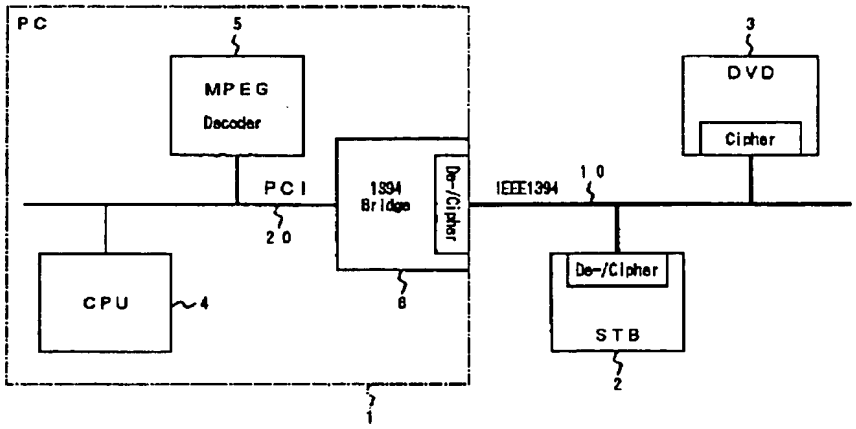
【図１０】


MPEG2
デコーダ
115
Plain Text
111
CPU
1151
Kcontrol
Authenticator
Kcontents
De-Cipher
1152
PCI
100
・eKcontrol
・eKcontent
1161
Authenticator
・Kcontent
・Encrypted
Contents
116
DVD－RAMドライブ

【図１４】


システム属性情報を取得
S201
ストリーム属性情報を取得
S202
システム属性情報とストリーム属性情報を比較
S203
S204
一致
No
Yes
S205
現在のストリームを処理
現在のストリームを廃棄
S206

【図１５】


PC
5
MPEG
Decoder
PCI
20
1394
Bridge
De-/Cipher
8
CPU
4
1
IEEE1394
10
3
DVD
Cipher
De-/Cipher
STB
2